Serious Cyberattack Raises Questions About GDPR Application in Finland

Susanna Lindroos-Hovinheimo 2020-11-05T17:31:45

Personal data about patients has been hacked from the privately-run psychotherapy centre Vastaamo in Finland. Last week, blackmailers demanded 450,000 euros in bitcoins in exchange for not going public with the data. The blackmailers proceeded to publish the files of 100 of Vastaamo's patients on the anonymous Tor network and claimed they would continue to publish every day until they received the ransom. The published data includes highly intimate information about patients' personal lives and mental health issues. Because of the seriousness of the breach, the case is likely to become a landmark in Finnish data protection law and a Europe-wide reference point for the application of GDPR rules in data breach situations.

According to recent media reports, the Vastaamo has already been hacked in 2018 and 2019, leading to serious suspicions of negligent data protection on the company's part. Vastaamo has around 20 clinics across Finland and tens of thousands of customers but it remains unclear how many of them have been affected by the data hack. The private company is also a subcontractor to several major public-sector hospital districts and employs about 300 psychotherapists. Now, the National Bureau of Investigation is investigating the case under criminal law as Aggravated Data Theft. The national data protection authority, the Office of the Data Protection Ombudsman, is also investigating the case.

Protecting patient data: Vastaamo's liability

The case raises various legal issues and displays the tendency of modern juridical problems to spread out into many different legal fields. The most important questions in this case stem from criminal law, data protection law and torts. The perpetrators, if they can be identified, are likely to face criminal charges. The Finnish Criminal Code includes several offences that may become relevant, the most important ones being Data Theft and Data Breach.

The main difference between criminal law and data protection law sanctions is that the criminalisation of Data Breach, which would be the offence in this scenario, does not include legal persons. Only natural persons can be held responsible. Therefore, the main legal framework for considering the liability of Vastaamo is provided by the General Data Protection Regulation (GDPR) and the national Data Protection Act. This case illustrates the strong role of current data protection law, which was amended and harmonised in the EU in 2018.

A potential landmark case for the application of the GDPR

Considering the scope and seriousness of the breach, and the amount of publicity it has gained, the case may become a landmark in Finnish data protection law. It needs to be established whether Vastaamo as the data controller has acted in accordance with data protection rules. If an infringement has occurred, Vastaamo can be ordered an administrative fine under Article 83 of the GDPR. There is not much case law on such fines in Finland, so the decision will become important for future legal assessment. Depending on the outcome of the case, it may become a model for the application of GDPR rules on a European-wide scale, as the Court of Justice of the EU (CJEU) has not yet delivered any authoritative ruling that would clarify the application of GDPR sanctions on a hacked company.

Article 83 of the GDPR has a lot of detail that needs to be assessed. Firstly, it is important to note the beginning of the Article, according to which the administrative fine shall in each individual case be “effective, proportionate and dissuasive.” The last word is illustrative. It shows the important aim of the fines: they are meant to have a pre-emptive effect. For this reason alone, if a fine is imposed on Vastaamo, it may be a large one.

Other factors that come into play when the size of an eventual fine is considered are, according to Article 83, the nature of the data, the large number of data subjects that have been affected, and the level of damage suffered by them. In this case, these all highlight the seriousness of the breach. The data is very sensitive, including patients’ diagnoses as well as names, addresses and national identity codes, and the number of victims has by the time of writing risen to an estimate of 15 thousand. Nevertheless, the level of damage is difficult to predict.

When considering whether Vastaamo should be fined, it is necessary to evaluate if the company has acted in accordance with data protection rules. Article 35 of the GDPR requires that controllers conduct a data protection impact assessment when their processing is likely to result in a high risk to the rights and freedoms of natural persons.The purpose is to identify and manage the risks related to the processing of personal data. According to Article 35(3) GDPR, such an impact assessment is required especially when processing health data. The Data Protection Ombudsman is currently investigating whether an impact assessment has been made by Vastaamo.

Further, it appears that the company has neglected to notify the victims that their data has been hacked. According to Article 34, when a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay. If the first data breach happened in 2018, it seems obvious that the company has neglected this requirement.

A company’s responsibility to pay compensation

It is clear that the hacking has caused mental suffering for the victims but it has also caused practical harm: The victims have to ensure that their data is not being used for identity theft or other malicious ends. The company may become liable to pay compensation to the victims. Under Article 82 GDPR, anyone who has suffered material or non-material damage as a result of an infringement has the right to receive compensation from the controller for the damage. In this regard, too, the case may become a trailblazer in Finland. Because of the peculiarities of the case, it may prove difficult to assess the non-material damage. It is hard to put a price tag on the suffering of the victims.

Compensation is a difficult issue in data protection law generally. Data is not like property. My data can be hacked, stolen, distributed and sold, but it is still my data. In the Vastaamo case, the intimate personal information that the blackmailers have published have now spread beyond anybody’s control. There is no way of getting the data back, or erasing it. Therefore, the victims can only receive compensation for suffering, harm and inconvenience. One factor that complicates things is time. The data is likely to circulate on various networks for a while causing harm. A fair and just amount of compensation in such a situation is impossible to assess.

If it becomes clear that the company has not followed the binding data protection rules, a further issue to consider is the employees. The personal data of one person can simultaneously involve personal data of another. This has been discussed by the CJEU for instance in the Nowak case (Case C-434/16). It is possible that the data leaked includes personal data of the therapists, for example their names and case notes including subjective impressions. The legal status of the employees has received almost no attention in the discussions pertaining to the data leak but may become relevant in the authorities’ assessments of Vastaamo’s liability.

Clarification of European data protection rules

This cyberattack has inflicted suffering on both the victims and Vastaamo’s employees. The negative media attention also hurt Vastaamo’s reputation significantly. The data breach highlights the importance of data protection and cybersecurity. Data protection is not only about the privacy of individuals. The rules benefit society much more broadly. And as this case shows, following data protection rules is also in the own interest of companies and other data controllers.

The outcome of the various pending legal proceedings connected to the hacking will provide much-needed clarification for the law. The European data protection rules form a relatively young area of legislation, where new authoritative interpretations continue to shape the meaning of the law. As this case will prove to be a complex one, rulings that will follow may help to clarify controllers’ liability as regards administrative fines as well as compensation to victims.

(cc) BY-SA